Les Guides Métiers de la MCEF

LES MÉTIERS DE LA CYBERSÉCURITÉ

Maison commune Emploi Formation PORTET-MURETAIN

SOMMAIRE

Présentation du secteur d'activité

Définition de la cybersécurité

D'après le site internet France Diplomatie, la cybersécurité recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre les cyberattaques que sont:

- Les utilisations criminelles d'internet (cybercriminalité)

- L'espionnage à visée politique ou économique

- Les attaques contre les **infrastructures critiques** (transport, énergie, communication…) à des **fins de sabotage**

L'augmentation spectaculaire du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des pays développés à renforcer leur résilience et à adopter des stratégies nationales de cybersécurité.

Les orientations stratégiques prises ces dernières années au plus haut niveau de l'Etat français ont consacré la cybersécurité comme l'une des priorités de l'action gouvernementale, en particulier à travers le discours de Jean-Marc AYRAULT en 2014.

Les entreprises de toutes tailles sont également sensibles à ces attaques et mettent en place des stratégies de lutte pour y répondre.

L'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** précise que la cybersécurité est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

La cybersécurité : une filière en plein développement

Présentation

La Branche est constituée de près de 60 000 entreprises adhérentes, représentant environ 750 000 emplois. Ces entreprises présentent une forte diversité tant en termes de taille (de très grands groupes mais aussi de nombreuses PME, plus de 50 000 entreprises ont moins de 2 emplois) qu'en termes d'activités adressées (secteur de l'énergie, de l'immobilier et de la construction, de la distribution, du commerce en ligne…).

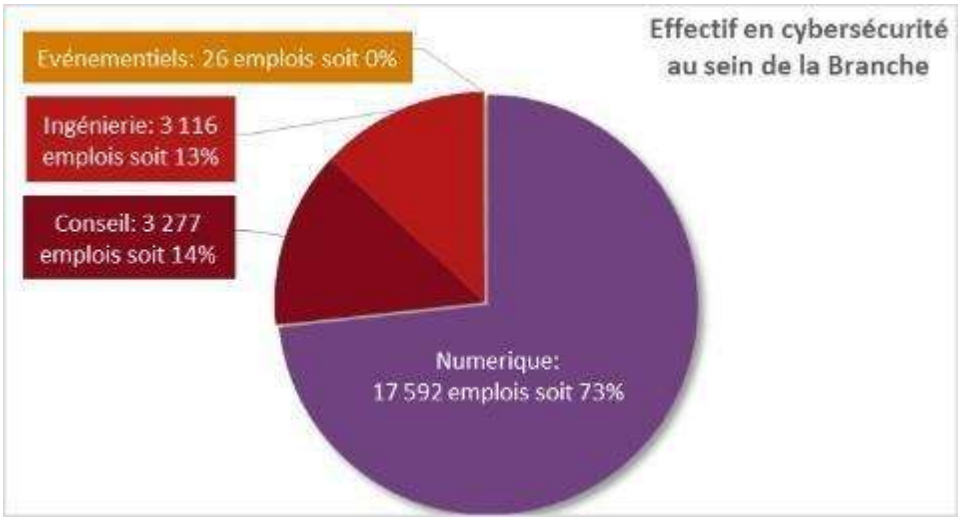
Source : Etude de l'OPIIEC

Les besoins en recrutement et en compétences

Les professionnels de la cybersécurité pour les entreprises de la Branche, correspondent aux personnes dont le cœur de métier est :

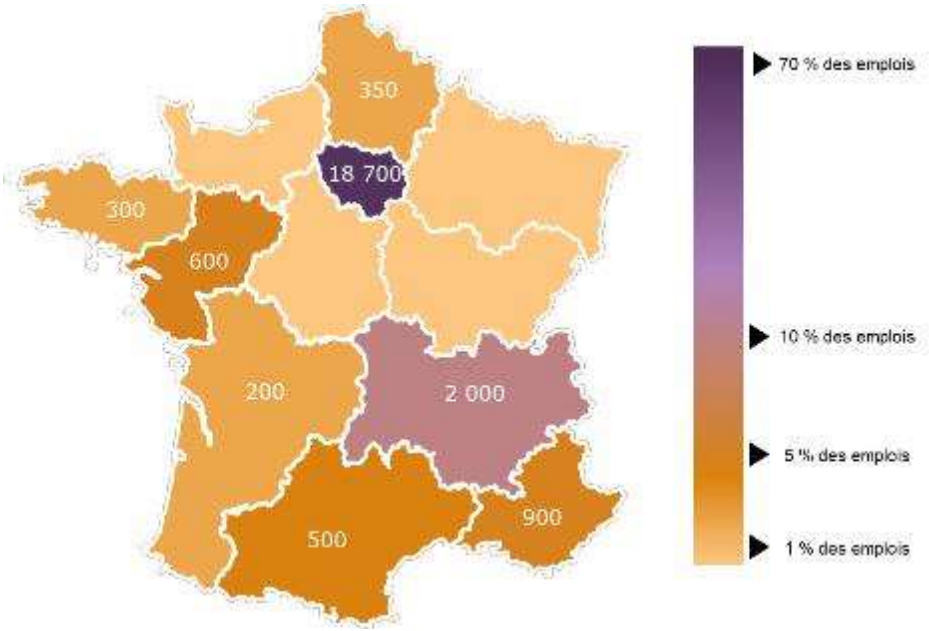
- Le développement de logiciels de sécurité tels que les antivirus, les anti-spams…
- La réalisation de prestations d'audit et de conseil en cybersécurité
- Le développement et l'intégration de solutions de sécurité telles que la gestion des identités et des accès (IAM), la prévention des pertes de donnée (DLP),…
- Les services managés de sécurité tels que le Centre des opérations de sécurité (COS ou SOC)

Avec plus de 24 000 emplois en cybersécurité au sein des entreprises de la Branche, les professionnels de la cybersécurité représentent ainsi 3% de l'effectif total des entreprises de la Branche (tous secteurs confondus). 24 000 emplois en cybersécurité au sein de la Branche font de cette dernière un ensemble important d'acteurs de la filière cybersécurité au niveau de la France.



REPARTITION DES EFFECTIFS AU SEIN DE LA BRANCHE SUIVANT LE TYPE D'ACTIVITE EN CYBERSECURITE

La carte de France ci-dessous donne une approche géographique des emplois en cybersécurité pour les entreprises de la Branche :



REPARTITION GEOGRAPHIQUE DES EFFECTIFS CYBERSECURITE AU SEIN DES ENTREPRISES DE LA BRANCHE

Ces emplois sont principalement situés en région Ile-de-France. Ce déséquilibre régional Paris-Province s'explique notamment par :

- Une forte présence des entreprises de la Branche en Ile-de-France (plus de 60% des effectifs)
- Un rattachement fréquent des fonctions en cybersécurité au siège des entreprises, majoritairement implanté en Ile-de-France

La région **Occitanie se place cependant au 5ème rang**, ce qui signifie qu'elle propose des débouchés importants pour les personnes souhaitant travailler dans ce domaine.

La cybersécurité constitue une filière d'avenir. Un million de postes sont à pourvoir à l'échelle mondiale.

Dans le cadre de ce marché qui se structure en France, encouragée par les nouvelles technologies et poussée par la montée en puissance des attaques internet et leur médiatisation, la cybersécurité pourrait, à terme, représenter une vitrine de la compétitivité des entreprises françaises.

Ces mises en conformité et les volontés indépendantes de montée en sécurité de leurs systèmes engendrent pour les entreprises des besoins forts en termes de cybersécurité.

La croissance du marché va donc se poursuivre. Cela se traduit par une demande forte, et des attentes croissantes des entreprises en termes de logiciel, matériel et prestations (conseil, formation…).

Plus spécifiquement, le marché français des appliances et des logiciels dédiés à différentes problématiques de cybersécurité (gestion de la sécurité, des accès ou des identités…) devrait progresser de 6,5% par an jusqu'en 202027. Une part de cette croissance de marché serait alors portée par la croissance des effectifs dans le secteur.

A horizon 3 ans, les entreprises de la Branche anticipent une croissance des effectifs en cybersécurité de 6 %, représentant 1 400 créations nettes d'emplois.

A horizon 5 ans, la tendance de croissance (création nette d'emplois) s'est vue confirmée par les entreprises avec une perspective de croissance de 8 %.

Si les grands groupes ont aujourd'hui conscience des risques et intégré les problématiques en cybersécurité à leur stratégie d'entreprise, ce n'est pas encore le cas des TPE-PME. Pour ces dernières, les choses avancent plus lentement.

Encore non équipées ou mal protégées, les petites entreprises constitueront vraisemblablement l'un des enjeux fort pour la cybersécurité, et représentent en ce sens un potentiel de croissance important pour la filière.

Un autre facteur de croissance à plus long terme réside dans la forte expansion des objets connectés, considérés parmi les priorités des entreprises en matière de digital. A l'horizon 2020, le monde sera équipé de quelques 21 milliards d'objets connectés. Leur sécurité va devenir un enjeu pour les années à venir.

Des initiatives autour de la cybersécurité en Région OCCITANIE

La multiplication des événements cybersécurité, contribuent à l'attractivité de la filière et constitue un autre processus de recrutement.
La **région Occitanie** n'échappe pas à la règle et voit fleurir de **nombreuses initiatives autour de la thématique de la cybersécurité**.

◇ *Les Rencontres Cybersécurité*

Les 6 et 7 juillet 2017 s'est déroulée la troisième édition des rencontres Cybersécurité et Territoires à Fleurance (Gers).
L'objectif est de rencontrer et sensibiliser les visiteurs aux risques liés à l'usage de l'informatique et faire connaître les bonnes pratiques pour la sécurité du numérique.
L'originalité de cette manifestation est de traiter des questions de cybersécurité à l'aune des **préoccupations des territoires péri-urbains et ruraux**.

◇ *Cyber@Hack : un événement dédié à la cybersécurité*

Le 21 septembre 2017 a eu lieu à Toulouse le 4ème Cyber@Hack avec pour thématique principale l'**innovation en matière de cybersécurité**.
Cet événement est organisé par PRISSM, un cercle de réflexion porté par Trust et Epitech.

◇ *Lancement du pôle OCSSIMORE le 1er mars 2017*

Dédié à la **recherche de solution pour la sécurité digitale**, ce pôle a officiellement été lancé autour d'acteurs de la sécurité et de l'entreprise (Pierre Fabre, l'école Epitech et Météo France sont déjà impliqués dans le projet).
Ocssimore est un groupement d'entreprises spécialisé sur les questions de sécurité digitale hébergé par la Banque Populaire Occitane.

◇ *Les Rencontres Cybersécurité Occitanie*

La 3ème édition de ces rencontres organisées par la Région et Touleco a eu lieu le 10 mai 2017.
Elles sont l'occasion de sensibiliser le public sur les besoins de plus en plus importants en matière de cybersécurité, face à des menaces croissantes. Les entreprises d'Occitanie, et notamment les sociétés industrielles, sont particulièrement concernées.

◇ *PRISSM (Professionnels de l'Industrie numérique de la Sécurité et de la Sûreté du Midi)*

PRRISSM est un Think Tank sur la cybersécurité rattaché à Digital Place et Aérospace Valley.
Crée par la Région Occitanie en collaboration avec MADEELI, il vise à réunir tous les professionnels et décideurs, les clubs et associations de la cybersécurité de la région.

Son objectif est de **développer le marché et la présence des acteurs régionaux**, leur **visibilité** et mettre leur croissance au service de la **création d'emplois et de richesses**.

◇ *Le projet de lancement d'un centre technique de la cybersécurité*

La Région Occitanie travaille actuellement sur l'ouverture d'un **espace de démonstration de l'offre régionale en matière de cybersécurité**.

La création d'un centre technique de la cybersécurité à destination des TPE et PME, a été annoncée lors de la 3e édition des Rencontres Cybersécurité Occitanie.

"Ce centre technique serait un **lieu dans lequel seraient mutualisés tous les outils de cybersécurité disponibles dans la région**. Il permettrait à toutes les TPE et PME, de tous les secteurs d'activités, d'**améliorer leur système informatique afin de protéger au mieux leurs données**. Ce type d'entreprises n'ayant que très rarement les moyens de s'offrir ces services, contrairement aux grands groupes. Les bénéficiaires pourraient également y faire **certifier leurs innovations**", dévoile Nadia Pellefigue la vice-présidente de la Région Occitanie.

Les métiers de la cybersécurité

Fiches Métiers

L'ANSSI, avec un groupe de travail composé de représentants de l'enseignement supérieur et du monde industriel, propose de structurer les métiers de la cybersécurité autour de 16 profils

Cette liste permet d'identifier plusieurs nouveaux cœurs de métiers actuellement en plein développement :

Pour accéder à ces formations, il est recommandé d'avoir des **pré-requis** solides en architecture réseau, langages informatiques (Python) et droit.

Technicien support (niveau BTS/IUT)

Le technicien support est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou administratifs : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets.
Selon le profil d'emploi et la formation reçue, il est en mesure de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements serveurs et des terminaux traitants. Il est en capacité d'effectuer des tâches de contrôles administratifs de conformité dans le domaine des habilitations du personnel, du suivi comptable et des inventaires réglementaires, de l'application des procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle. Il contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux. Dans le domaine de la cybersécurité, le technicien veilleur analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités.

Auditeur, contrôleur, évaluateur (niveau master)

L'**auditeur** ou le **contrôleur** couvre un champ d'application vaste composé de plusieurs domaines complémentaires. Si la finalité recherchée est globalement traitée par les Centres d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) pour les logiciels et matériels, les audits terrain sont effectués par des experts en règles d'installation et de déploiement/usage, requérant un audit in situ pour les systèmes ou équipements déployés et logiciels paramétrés. Le spécialiste de l'audit ou du contrôle recherche :
la conformité, si requise, au plan réglementaire (contrôle des règles d'installation pour l'homologation ou la ré-homologation) ;

les vulnérabilités susceptibles de contourner les mécanismes de sécurité en conception ou en mode déployé afin d'éviter les compromissions de données ou d'éléments de protection.

Post-auditeur (niveau master)

Le **post-auditeur**, architecte de sécurité expérimenté et certifié « système ou réseau », établit la cartographie et oriente les investigations des équipes d'analyse dans un contexte difficile. Il intervient sur sollicitation à la suite d'un audit, d'un incident ou d'une intrusion, prend la mesure de la situation et propose un plan de remédiation. Conjointement à l'élaboration du profil de l'agresseur et à son éviction du système, il aide à produire les informations qui seront nécessaires pour les activités aval de remédiation avec les potentiels impacts métiers, pilotant les équipes et rendant compte.

Ses compétences et son expertise des solutions lui permettent de dialoguer efficacement avec les interlocuteurs et experts techniques dans le(s) domaine(s) touché(s), qu'il mobilise en tenant compte de la culture de l'entreprise. Il propose les mesures techniques et processus palliatifs prioritaires à court terme.

Opérateur (niveau master)

L'opérateur, selon le domaine concerné (mise en service ou soutien d'équipements de sécurité, supervision, gestion d'attaques…) met en œuvre la politique de sécurité de l'information, contrôle et prend des mesures contre les intrusions, les fraudes, les atteintes ou les fuites concernant la sécurité. Il garantit l'analyse et la gestion des évènements concernant la sécurité des données et des systèmes d'informations de l'organisme, il passe en revue les incidents de sécurité et formule des recommandations pour une amélioration continue de la sécurité.

Intégrateur (niveau master)

L'intégrateur de sécurité système analyse et prend en charge les volets sécurité (objectifs, niveau de criticité et attentes en termes de résilience) en liaison avec l'architecte des projets informatiques et programmes dans l'infrastructure. Il définit et met en œuvre des plates-formes nécessaires à l'intégration des solutions (services ou produits de sécurité) dans les nouvelles applications. Il planifie, coordonne, en relation avec les autres secteurs concernés (réseaux, système de gestion base de données, etc.), les besoins d'intégration exprimés. Il installe des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires dans un système existant ou en cours de développement, respecte les processus et procédures établis (i.e. gestion de configuration) en tenant compte de la spécification, de la capacité et de la compatibilité des modules existants et des nouveaux modules afin de garantir intégrité et interopérabilité.

Il contribue à la qualification technique et à l'intégration dans l'environnement de production. Il documente les processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité et organise les conditions de mise en œuvre du maintien en condition de sécurité.

Formateur, instructeur (niveau master)

Il participe à (**formateur**) ou est responsable de (**instructeur**) la formation ou la sensibilisation du personnel sur les volets réglementaires, techniques ou opérationnels de la SSI et de la cybersécurité. En mesure de mettre en place des travaux pratiques sur les produits et réseaux, il pourra animer des équipes attaque/défense sur des plates-formes d'entraînement représentatives des domaines de l'informatique classique ou des automates industriels, simulant en temps contraint la réponse à des attaques ou incidents de sécurité. Cette tâche est confiée aux formateurs et instructeurs les plus expérimentés.

Disposant d'une expérience technique ou opérationnelle dans les domaines enseignés (administrateur, opérateur, réglementation, technique), il se tient informé de l'état de l'art dans son domaine et assure une veille active permettant d'actualiser ses cours en fonction de l'évolution du contexte (technique, menaces, régulation). Titulaire de références pédagogiques, il veille à illustrer ses cours de travaux pratiques, démonstrations ou exercices participatifs.

Développeur de sécurité (niveau master)

Le **développeur de sécurité** assure le sous-ensemble des activités d'ingénierie nécessaires à la réalisation d'éléments, de produits, de logiciels répondant à des exigences de sécurité, en cohérence avec les objectifs qui leur sont alloués et une définition d'architecture d'ensemble. Le spectre de ces éléments, produits et logiciels comprend : design, interfaces, spécification, conception, codage, production de binaire, assemblage, test, préparation à l'intégration de niveau solution, gestion de sources, gestion de configuration, gestion des faits techniques, archivage, documentation.

Il développe de façon méthodique, en appliquant des règles de conception / codage / tests (qu'il définit au besoin ou qu'il contribue à définir) et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse (tests aux limites et hors limites), de sécurité (résistance aux attaques identifiées en entrée de la conception), et de performances. Il s'assure de l'applicabilité des licences des solutions qu'il utilise, et au besoin de l'innocuité de leurs composants.

Architecte de sécurité (niveau master)

L'**architecte de sécurité** structure les choix techniques, technologiques et méthodologiques d'un ensemble (système d'information, logiciel) répondant à des exigences de sécurité, en cohérence avec les activités équivalentes réalisées au niveau de la solution qui l'intègre. Il s'assure de la déclinaison optimale des exigences techniques d'entrée (fonctionnalités à offrir, contraintes de performance, d'interopérabilité, d'interchangeabilité, de robustesse, d'intégration de solutions sur étagère, d'exportabilité), selon des critères de coût, d'efficacité, de stabilité, de maîtrise, de niveau de risque, de respect des standards, d'aptitude à la production, au déploiement et à la maintenance MCO (maintien en conditions opérationnelles) et MCS (maintien en conditions de sécurité).

Il identifie et valide la cartographie du système d'information et notamment s'assure que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception. Il veille à ce que les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire soient effectivement déclinées. Il fournit la connaissance de l'état de l'art des architectures prenant en compte les développements futurs et il prépare les dossiers de conception et de justification.

Expert en sécurité des systèmes d'information (niveau master)

L'**expert en SSI / cybersécurité** est en capacité de traiter des dossiers complexes (périmètre d'envergure ou spécificité technique poussée). Ses connaissances approfondies des référentiels de sécurité, réglementations, produits et systèmes lui permettent d'instruire des dossiers de sécurité et de les soutenir auprès des acteurs du domaine (administration, instances de régulation, CESTI).
Ses capacités pédagogiques et rédactionnelles lui permettent d'élaborer des argumentaires techniques détaillés, voire de proposer de nouveaux développements pour constituer ses dossiers. Sa connaissance des solutions techniques lui permet d'argumenter sur les spécifications de sécurité avec des développeurs et des intégrateurs, en charge de définir et d'implémenter les architectures. Une expertise sécurité ciblée peut couvrir l'ensemble des fonctionnalités d'un produit ou de logiciels complexes d'éditeurs ou encore des domaines spécifiques comme les noyaux ou protocoles autour des métiers de l'embarqué, la téléphonie sur IP, les multiples technologies associées au *cloud computing* voire aux systèmes nouveaux (systèmes d'armes, systèmes de contrôle industriels…).

Expert des tests d'intrusion (niveau master)

L'**expert des tests d'intrusion,** ou « hacker éthique », est en mesure de pénétrer le système d'information et d'identifier les divers chemins d'intrusions, les techniques classiques ou atypiques utilisées, traçant ainsi le profil (*profiling*) des attaquants, leurs habitudes et méthode de travail (accès, dépôt, exfiltration, habitudes, périodicité…).

Il connaît les principes de protection des produits de sécurité, leurs limites voire leurs méthodes de contournement. Se tenant informé grâce aux forums ad hoc et revues spécialisées, il est en mesure de développer des scénarios d'intrusion à l'état de l'art et peut se spécialiser sur certaines cibles techniques (systèmes d'exploitation, téléphonie sur IP, protocoles réseau, etc).

Analyste (niveau master)

L'analyste peut contribuer à plusieurs domaines d'activités de la cybersécurité, dans les domaines de :

l'anticipation technologique avec de la veille technique ;

l'anticipation dans le domaine du renseignement sur les menaces, avec de l'analyse d'impact des codes d'exploitation (activités CERT et intégrateur de solutions) ;

l'anticipation en conduite pour évaluer les dommages subis par un système compromis, participer à la conception de la solution technique visant à restituer le service et apporter ses compétences de spécialiste en matière de mise en œuvre des principes de sécurisation SSI et dans le domaine technique de la cyber sécurité.

Il peut contribuer au schéma directeur et à l'urbanisation sécurisée des systèmes.

Consultant (niveau master)

Le **consultant sécurité** anticipe et fait mûrir la prise en compte des enjeux de sécurité dans les organisations. Il alimente les nouveaux projets par une analyse des dispositifs existants et une sensibilisation aux problématiques de cybersécurité (menaces, vulnérabilités, analyse du marché) liées aux technologies en rapport avec une analyse prospective des processus métiers.

Il assiste la direction ou la maîtrise d'ouvrage dans la définition des besoins, de la politique et des solutions de sécurité à mettre en œuvre, en veillant à améliorer l'intégration de la sécurité dans le système d'information d'entreprise. Ses actions consistent en :

- prescrire recommander des pistes pour le développement et la mise en œuvre de la sécurité d'une organisation, d'un projet ou d'une solution ;
- participer à la définition des processus, des spécifications générales des projets ;

- vérifier la cohérence de l'architecture applicative et fonctionnelle et de son évolution ;
- participer si besoin à l'évaluation et au choix d'une solution de sécurité ;
- assister les métiers ou la maîtrise d'ouvrage pour le développement de la sécurité du projet ;
- effectuer des préconisations de management garantes de la cyber résilience dans le cadre de l'accompagnement d'un projet.

Spécialiste en gestion de crise (niveau master)

- Le **spécialiste en gestion de crise** cyber conseille l'organisme pour lui permettre de disposer d'une capacité de gestion de crise majeure dédiée aux systèmes d'information, ou avec un volet cyber prépondérant. Il organise la gestion de crise pour :
- agir et résoudre la crise ;
- communiquer l'état de la crise aux personnes et aux organismes concernés ;
- coordonner l'action des différentes parties en présence.
- Il limite les volets organisationnels, l'entraînement et la simulation aux acteurs susceptibles d'intervenir en cas de crise majeure liée aux systèmes d'informations et à leurs interlocuteurs métiers ou support concernés à contacter (gestionnaire de crise, RSSI, responsables de l'ingénierie, administrateurs systèmes / données). À un autre niveau plus technique et sous la pression d'une attaque en cours, le profil de gestionnaire de crise technique peut être également identifié.

Expert connexe (niveau master)

- Nouveau profil d'expert, né de la nécessité de coordination des techniques de cyberdéfense et de résilience (continuité d'activité métier) face aux attaques, il dispose d'une double compétence et expérience dans les deux domaines. Indifféremment issu de la SSI ou de l'un des secteurs concernés (énergie, télécom, finances, etc.), il a pour rôle essentiel d'analyser, de concevoir, d'intégrer ou de mettre en œuvre, selon son périmètre d'action, les technologies de sécurisation dans le cadre de son domaine métier et des enjeux afférents. Maîtrisant les référentiels respectifs, il est en mesure de :

- faire converger les objectifs de sécurité et de sûreté de fonctionnement,
- conduire des analyses de risques en rapport
- proposer les solutions de résilience optimales, afin de minimiser sans concession les impacts métiers, face à l'installation définitive de la menace cyber dans les entreprises et l'Administration.
- Conseiller des directions métiers, il contribue à l'expression de besoin globale et technique de sécurité en conception, en intégration et en gestion de la sécurité.

Juriste spécialisé (niveau master)

- Le **juriste spécialisé** en cybersécurité est un expert du droit des technologies de l'information et de la communication qui s'est spécialiste des thèmes et des corpus concernés par la cybersécurité, la cybercriminalité et la protection des données à caractère personnel. Il peut opportunément présenter une expérience d'avocat à même d'éclairer la direction sur les conséquences pénales ou civiles d'une cyberattaque, dès lors qu'une décision voire la gestion d'une crise avec une composante cyber requiert son expertise.
- Conseil de la direction en matière de responsabilités civile et pénale, il se tient informé des évolutions de la réglementation internationale, européenne et nationale. Il effectue une veille juridique depuis le simple projet jusqu'à la publication et l'entrée en vigueur des textes régissant les conflits armés, le droit des affaires (notamment le secret des affaires), ainsi que la jurisprudence, en différenciant selon que la décision soit un cas d'espèce ou au contraire amène des réflexions plus générales sur la pratique du droit.

Responsable de la sécurité des systèmes d'information (niveau master + expériences)

Le **responsable de la sécurité des systèmes d'information** se charge de proposer à l'autorité compétente la politique de sécurité du SI et de veiller à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir en matière de SSI sur tout ou partie des systèmes informatiques et télécoms de son entité, tant au niveau technique qu'organisationnel. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose les évolutions qu'il juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.

Community Manager spécialisé en e-réputation

Le **Community Manager spécialisé en e-réputation** intervient en complément des autres professionnels de la cybersécurité pour gérer la situation de crise générée par la cyber attaque.

Le correspondant informatique et libertés

Le **correspondant Informatique et Libertés** (CIL) veille à la bonne application, dans l'organisme qui l'emploie, de la loi "Informatique et Libertés" de 1978 modifiée en 2004, relative à la protection des données personnelles et bientôt du règlement européen (2018).

La première mission du CIL est de faire respecter la lettre et l'esprit de la loi Informatique et Libertés par l'organisme qui l'emploie. Il veille à la sécurité des données personnelles contenues dans les bases de données de tous les services de l'organisme et à leurs conditions d'utilisation.

Il doit garantir la transparence et le caractère licite des traitements de données. Ces données peuvent concerner le personnel de l'organisme, mais aussi ses clients et ses usagers, et toute personne concernée par son champ d'activité.

Le CIL signale à son responsable tout manquement à la loi et dresse un bilan de son activité tous les ans. Il est l'interlocuteur privilégié de la Cnil (Commission nationale de l'informatique et des libertés).

Parallèlement, le CIL doit aussi former le personnel de l'organisme à la législation Informatique et Libertés. Ce double rôle exige à la fois de la fermeté et de la diplomatie.

Source : https://www.ssi.gouv.fr/particulier/formations/profils-metiers-de-la-cybersecurite/

Formations

La formation dans la cybersécurité en France

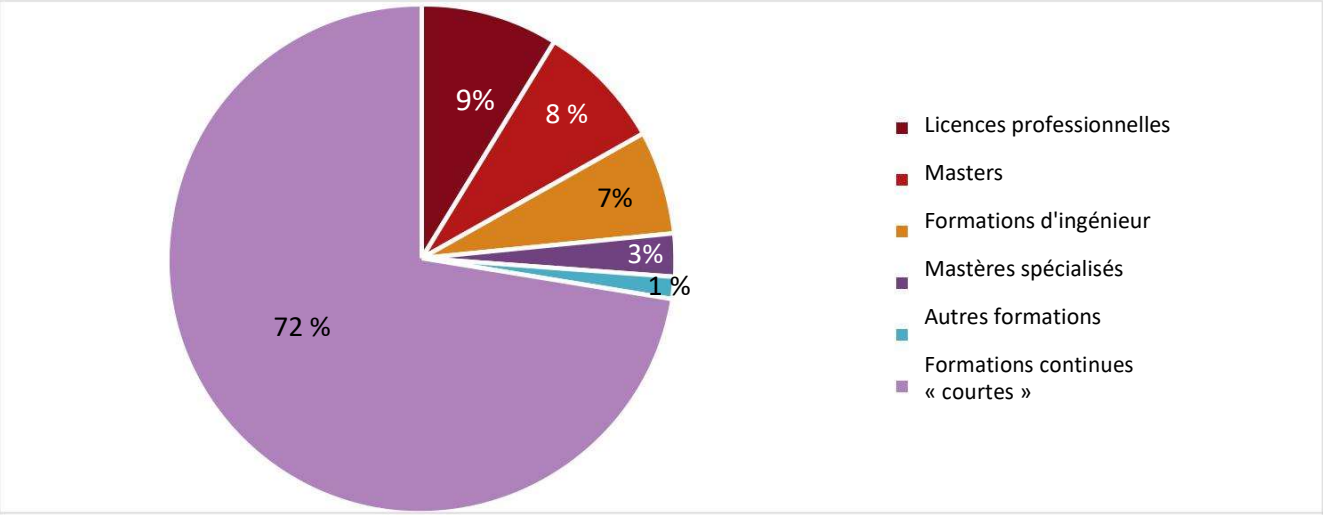
Au total, plus de 550 formations ont été identifiées par l'OPIIEC, avec une forte diversité en termes de durée (formations courtes et formations longues) et en termes de structures formatrices, allant des établissements d'enseignement supérieur aux organismes de formation privés.

L'OPIIEC a recensé la plupart des formations en cybersécurité en France, classées en 8 catégories :

Près de 150 formations dispensées par des établissements d'enseignement supérieur :

- 48 licences professionnelles
- 45 masters
- 37 formations d'ingénieur
- 15 mastères spécialisés
- 8 autres formations (type BADGE67, bachelor…)

- 242 formations techniques
- 102 formations en management de la sécurité
- 46 formations d'audit
- 15 formations en sécurité juridique



REPARTITION DES FORMATIONS EN CYBERSECURITE PAR TYPE DE FORMATION

Cette cartographie n'a pas vocation à être exhaustive de l'ensemble des formations françaises en cybersécurité, et n'inclut pas les formations dites de « sensibilisation » à la cybersécurité. Le focus est fait ici sur les formations professionnalisantes, proposant des cursus de qualité reconnus par les professionnels et les experts du secteur. Cet état des lieux a été réalisé de janvier à février 2017.

La formation dans la cybersécurité en Occitanie

Contacts des organismes de formation du Programme régional de formation professionnelle (PRFP) 2017
(Formations financées pour les demandeurs d'emploi)

• Master 2 Pro sciences et techniques des activités physiques et sportives mention STAPS : management du sport - Parcours Ingénierie Sécurité Sûreté Défense (ISSD)

Date : du **25/09/2017** au **21/09/2018**
Lieu : Université TOULOUSE 3 Paul Sabatier
Durée : **1190 heures**

Contact référent :
Mme Sandra JOFFROY
05 61 55 75 12
sandra.joffroy@univ-tlse3.fr

• Master 2 parcours sécurité des systèmes d'information et des réseaux (SSIR)

Date : du **25/09/2017** au **14/09/2018**
Lieu : Université TOULOUSE 3 Paul Sabatier
Durée : **1334 heures**

Contact référent :
M .Benzekri
05 61 55 60 86
abdelmalek.benzekri@univ-tlse3.fr

• Master 2 droit, économie, gestion mention science politique - Parcours type : Relations Internationales et politiques de sécurité

Date : du **07/10/2017** au **30/09/2018**
Lieu : Université TOULOUSE 1 Capitole
Durée : **560 heures**

Contact référent :
M. Bernard LABATUT
05 61 12 88 36
05 61 12 88 29
m2fcv2a@ut-capitole.fr

ZOOM sur le Master 2 ISSD Université Paul Sabatier

Ce Master, qui s'adresse à un public en **formation continue**, a pour objectif de donner aux salariés des secteurs public et privé de la sécurité, de la sûreté et de la défense, les moyens de prendre du recul par rapport à leurs grandes expériences du terrain opérationnel. Le principal objectif consiste à **considérer le domaine scientifique comme un aspect central de la formation**.

Ce Master permet donc de répondre aux deux grandes actions de la formation continue dans le cadre de la Formation Tout au Long de la Vie (FTLV) en y intégrant l'ensemble des situations où s'acquièrent des compétences : actions de formation continue, activités professionnelles, implications associatives ou bénévoles.
Cette formation inclut ainsi les démarches d'orientation, de bilan, d'accompagnement vers l'emploi, de formation et de validation des acquis de l'expérience.

Ce Master a donc pour objectif de **former des professionnels susceptibles d'occuper des emplois de cadres** dans les domaines de la formation à destination des intervenants en situations hostiles et des institutions qui encadrent ces différentes missions.
Par la formation continue, les divers professionnels de ces secteurs, bénéficient également d'une possibilité de poursuite d'étude leur permettant d'accéder à une reconversion dans le monde du travail (cas des Officiers sous contrat, retraité militaire etc….).

Cette formation a pour finalité de développer les compétences professionnelles (par une immersion à visée opérationnelle), afin que les professionnels puissent étendre leurs champs de compétences dans le cadre de leurs fonctions et/ou tenir le rôle de responsables pédagogiques, de responsables de formation ou d'experts de l'analyse des pratiques dans les domaines spécifiques de la sécurité, de la sûreté et de la défense et de répondre aux attentes des entreprises (PME et grandes entreprises) en matière de sécurité informatique, protection des données etc....

Tous les enseignements sont enregistrés en audio et une plateforme pédagogique est également accessible à tous les stagiaires inscrits au sein de ce MASTER pour la transmission des divers contenus de la formation (cours, comptes-rendus de séminaires...).

Le nombre de diplômés varie entre 92 et 100% chaque année. Cette différence est due au fait que plusieurs stagiaires effectuent le MASTER 2 en deux ou trois ans (passage du mémoire l'année suivante) et que quelque stagiaires ne valident que certaines UE et pas le diplôme (valorisations de compétences professionnelles).

Programme du Master 2 ISSD

- Ingénierie des dispositifs de formations opérationnelles
- Ingénierie des compétences à la sécurité et théorie de la sécurité – sécurité économique et gestion de crise
- Droits et obligations en matière de sécurité
- Sécurité et Défense – Sécurité économique – Enjeux industriels géostratégiques
- Séminaire semestre 9 et Langue Vivante - anglais scientifique et opérationnel
- Sécurité, hygiène et santé au travail - Sécurité des Activités Physiques et Sportives – Politique de sécurité
- Sécurité et sûreté
- Sécurité des systèmes d'information (SSI) – Cybersécurité – Systèmes intelligents
- Séminaire semestre 10 et Langue Vivante - anglais scientifique et opérationnel
- Langue Vivante - anglais scientifique et opérationnel
- Mémoire et stage

Pour en savoir plus contactez la responsable du Master :
JOFFROY Sandra
sandra.joffroy@univ-tlse3.fr
Tél : 05 61 55 75 12

Témoignages

Sandra JOFFROY

Responsable du Master 2 Parcours Ingénierie Sécurité Sûreté Défense (ISSD) (Université Paul Sabatier)

Sandra JOFFROY

Comment est né ce Master ISSD ?

En Réponse au livre BLANC de 2008 afin de confronter les expériences entre le Ministère de la Défense et celui de l'Enseignement Supérieur et de la Recherche.

Comment peut-on intégrer le master ISSD ?

Par Validation d'acquis professionnels (VAP et VAE) et/ou après la validation d'un MASTER 1.
Les compétences en matière de sécurité, sûreté et défense sont prises en compte.
Les demandeurs d'emploi peuvent bénéficier d'un financement de la Région Occitanie.
La formation ne s'effectue qu'en formation continue, il n'y a pas de possibilité de la suivre en formation initiale.

Quel est le contenu de l'enseignement ?

Le contenu de l'enseignement est axé autour de connaissances et compétences diversifiées en ingénierie :
- Domaines sécurité, sûreté et défense
- Cybersécurité, Intelligence Economique, gestion de crise, ingénierie de formation….

Quels sont les débouchés (typologie de métiers, entreprises) ?

A l'issue de la formation, les personnes diplômées peuvent exercer les métiers d'officier de sécurité, responsable de formation, chargé de sûreté ou encore proposer leurs services en consulting et audit

Pour plus d'informations : http://www.univ-tlse3.fr/masters-/master-staps-management-du-sport-parcours-ingenierie-securite-surete-et-defense-667081.kjsp?RH=1455716845617

Fabrice CRASNIER

Responsable du pôle FORENSIC – Laboratoire SCASSI-CYBER

SCASSI
be secure

Quel a été votre parcours professionnel (ou de formation) avant d'intégrer le Master ISSD ?

Après 25 années passées au sein de la Gendarmerie Nationale dont 15 ans à traquer la cyberdélinquance au service de nos concitoyens, j'ai entrepris de poursuivre mes activités au sein d'une société d'experts conseils en cybersécurité.
Je suis ingénieur en conception et développement informatique et doctorant en intelligence artificielle, j'ai intégré la formation Master ISSD en 2014.

Que vous a apporté la formation ?

Le Master ISSD m'a apporté un nouveau regard sur les problématiques des sociétés et sur les besoins des intervenants en matière de sécurité informatique. Ce parcours s'adressant particulièrement aux professionnels de la sécurité, cette formation m'a permis de mieux échanger avec mes camarades. Etudier et enseigner avec des étudiants qui ont le recul nécessaire sur le travail et les parcours atypiques comme le miens a été une réelle satisfaction. En gendarmerie, nous vivons un peu en autarcie et le plus souvent reclus dans notre univers institutionnel bien que notre institution soit tournée vers les problématiques sociétales ce qui ne veut pas dire problématiques des entreprises.

La formation est très riche, d'une part par les activités transversales proposées sur l'ensemble du périmètre de la sécurité qui est vue à la fois par des institutions et par des professionnels de la sécurité des entreprises, et d'autre part lors des immersions dans les entreprises et dans environnements spéciaux. C'est cet ensemble de compétences qui sont par la suite reconnues par la future entreprise qui recherche de la flexibilité, de l'adaptation et de la polyvalence chez sa nouvelle recrue.

Quel poste occupez-vous actuellement ?

Actuellement j'occupe le poste de responsable du pôle Forensic (expertise en informatique légale) au sein de la société SCASSI Conseil.
Ma nouvelle société offre des prestations dans la conception et l'exploitation optimale d'infrastructures de sécurité.
Elle apporte également des conseils à chaque étape, depuis le diagnostic jusqu'à la mise en œuvre, le contrôle et l'amélioration des dispositifs, afin d'assurer de leur conformité vis-à-vis des réglementations et des politiques de gestion des risques.
Enfin, elle accompagne dans la définition et l'implémentation des exigences sécurité dans tout projet industriel jusqu'à l'obtention des homologations nécessaires comme la sécurité logicielle et embarquée (IOT) à laquelle nous ajouterons les activités d'expertise en informatique légale au sein d'un nouveau laboratoire SCASSI-CYBER.

Pouvez-vous nous décrire votre journée type d'expert en cybersécurité ?

Le matin, je commence par la lecture des articles et forums dédiés à la cybersécurité afin de prendre en compte les évènements de cybersécurité de la veille. Cette action est primordiale afin de toujours suivre les évolutions sur les attaques et sur les nouveautés. J'informe ensuite l'ensemble de mes collaborateurs susceptibles d'être intéressés par certains sujets.

Après cette veille sur les réseaux du cyberespace, je commence à prendre mon travail dans le laboratoire qui consiste à analyser des matériels informatiques (ordinateurs, serveurs, disques durs, téléphones, etc.) à l'aide d'outils ad hoc pour en extraire les preuves légales qui pourront servir aux règlements de litiges dont l'objet peut être numérique, ou servir de point de départ pour une action judiciaire devant le tribunal civil ou pénal.
A l'issue des opérations d'extraction, je dois rédiger un rapport technique qui servira de base au conseiller juridique de l'entreprise ou à l'avocat conseil pour commencer un travail de règlement. Ce rapport peut même servir de preuve lors d'un procès pénal.

La fin de journée est consacrée à la recherche et au développement pour nous permettre de rester toujours à niveau et pour rester plus efficient dans nos approches et nos procédures. Il est toujours bon de se remettre en question sur des problématiques tout en concevant de nouveaux outils pour nous aider à être plus efficace.

Témoignages

Alexandre GUIBARD

Formateur en secourisme et sécurité incendie, responsable logistique (Comité Français de Secourisme de la Haute-Garonne (CFS 31). Association de sécurité civile)

Quel a été votre parcours professionnel (ou de formation) avant d'intégrer le Master ISSD ?

Titulaire d'un baccalauréat Scientifique je me suis alors orienté vers un DUT HSE (Hygiène - Sécurité - Environnement) option Protection des Populations et Sécurité Civile pour poursuivre sur une Licence Professionnelle STAPS GCPSH (Gestion de la Condition Physique des Intervenants en Situation Hostile) afin de préparer au mieux un engagement futur au sein de l'Armée de Terre par le cursus Officier.

J'ai donc intégré le Master ISSD en ce sens grâce à la validation des acquis professionnels étant sapeur-pompier volontaire, nageur BNSSA et formateur en secourisme en parallèle de mes études.

Que vous a apporté la formation ?

Le master ISSD est une formation faite pour les curieux !
Ainsi des personnes sans compétences particulières en informatique et en cybersécurité côtoient des as en la matière et c'est ce qui fait sa force.
Le débutant sans vouloir devenir spécialiste va apprendre un langage commun, va être capable de comprendre les dangers du cyberespace et de ce qu'il est possible de faire dans nos sociétés modernes à partir d'un simple réseau wifi par exemple…
C'est à la fois déconcertant et très enrichissant.
D'une part, on prend conscience des travers de nos sociétés virtuelles et on apprend à s'en prémunir par des choses toutes simples, comme des « règles élémentaires » qui devraient être connues de tous.
Et d'autre part, des méthodes beaucoup plus complexes et toujours plus intéressantes qu'utilisent le gouvernement par exemple pour mener à bien ses enquêtes et combattre toutes les cyber-menaces actuelles.

Quel poste occupez-vous actuellement ?

Je suis actuellement formateur et responsable logistique pour une association de sécurité civile en matière de secourisme et de sécurité incendie le temps de préparer mon recrutement officier dans l'armée de terre pour l'année 2018.

Pouvez-vous nous décrire votre journée type d'expert en cybersécurité ?

Il est vrai que la cybersécurité n'est pas mon cœur de métier actuellement car elle n'est pas la raison pour laquelle j'ai été embauché à ce jour.

Toutefois, l'acquisition de ce master me permet au quotidien de sensibiliser mon entourage personnel (famille, amis…) victime parfois d'usurpation d'identité sur les réseaux sociaux par exemple, ainsi que mes collaborateurs de travail lorsqu'ils reçoivent des mails suspects par technique de « phishing » notamment.

Je suis en effet en capacité de leur donner des conseils à titre préventif, mais aussi des réactions réflexes à avoir lorsqu'il est « trop tard » pour « limiter les dégâts ».

Conseils aux entreprises en matière de cybersécurité

Major Fabrice CRASNIER

Commandant de la division Analyse Criminelles et Investigation spécialisées à la section d'appuis judiciaire de Toulouse (Gendarmerie Nationale)

Quels sont les enjeux de la cybersécurité pour les entreprises ?

Il y a quelques années (à l'échelle du temps de la construction du cyberespace c'est-à-dire il y a deux ans) les enjeux étaient essentiellement financiers, aujourd'hui, ils deviennent vitaux car ils sont en capacité de mettre en péril l'entreprise.
Dans le cadre de mes fonctions, j'ai eu à connaitre une grande quantité de faits délictuels provenant du cyberespace dont certains malheureusement viennent confirmer mes propos. Prenons le cas des faux ordres de virement internationaux communément appelé la fraude au président. Si certaines sociétés à la trésorerie solide ont pu faire face à cette escroquerie d'autres structures plus modestes comme des Scop (Sociétés coopératives et participatives) ou des associations ont dû fermer leurs portes.

Quelles sont les entreprises les plus touchées par les cyberattaques?

Les cibles sont très hétérogènes mais aujourd'hui nous pouvons dire que toutes les entreprises qu'elles soient répertoriées en tant que TPE, associations, PME, grands groupes, administrations sont toutes des cibles potentielles pour un cyber agresseur. En effet, à partir du moment où l'entreprise possède un système d'information connecté au cyberespace alors elle est susceptible d'être la proie d'actes malveillants.

Quelles sont les différents types d'attaques ?

Il n'est pas très difficile aujourd'hui de parler de ce sujet tant l'actualité a été riche pour ne parler que de 2017.
Depuis quatre ans, j'ai pu observer l'impact progressif des malwares de type rançongiciels (ransomware) sur l'environnement professionnel avec une farandole de faits cette années encore sur de grands groupes industriels que l'on pensait à l'abri de ces actes de malveillances. Ainsi, Renault, impacté par le malware Wannacry en mai 2017 a dû mettre au chômage technique durant une journée l'ensemble du personnel d'une chaine de montage, les réparations ont durée plusieurs semaines. Suite à cette attaque de masse, les observateurs ont dénombré plus de 200.000 entreprises

victimes sur le plan mondial ce qui en fait l'une des plus grandes pandémies virales de type informatique à ce jour.

Le groupe Saint-Gobain, victime du malware Not-Petya en juin 2017, a perdu plusieurs centaines de millions d'euros suite à cette attaque et vraissemblablement des données numériques perdues à jamais. Malheureusement le groupe Saint-Gobain n'a pas été la seule victime. Parmi les autres, nous pouvons citer la filiale immobilière de la BNP Paribas, Verallia le groupe spécialisé dans les emballages alimentaires en verre et Auchan le grand groupe spécialiste de la distribution. Même la SNCF dit avoir repéré des tentatives d'installation du virus sur son réseau, mais ne pas avoir été touchée. Tout cela pour ne parler que des entreprises françaises.

Les entreprises françaises sont-elles suffisamment conscientes des dangers et se protègent-elles correctement ?

La prise de conscience commence seulement à prendre forme mais la maturité n'est pas encore au rendez-vous. Les failles de sécurité qu'elles soient informatiques ou comportementales, sont encore trop nombreuses malgré des efforts constants depuis dix ans. Les nouvelles dispositions relatives au Règlement européen sur la protection des données (RGPD), aux entreprises d'importances vitales (OIV) et autres règlements spécifiques dans la santé ou la banque vont très certainement améliorer la maturité de l'entreprise et de ce fait sa sécurité informatique.

Pourriez-vous donner deux conseils aux entreprises pour se protéger ?

Le premier conseil serait de **prendre en compte la sécurité de son système d'information**[1] **(SI) comme un risque majeur** et non plus comme un outil renouvelable en cas de panne.
Ce n'est pas un ordinateur avec une obsolescence programmée. Il ne faut pas le confondre non plus avec le réseau informatique qui a pour rôle de vous donner accès au système d'information. La meilleure façon de vous en rendre compte est de couper l'usage informatique de votre entreprise, i.e. plus d'internet, puis plus de réseau interne et enfin plus de machines de bureau, à partir de cet instant seulement vous pourrez évaluer le risque de le perdre.

Le second conseil est de **bien comprendre que la sécurité informatique n'est plus une option dans une filière d'apprentissage**, « un vernis sécuritaire », mais une **filière à part entière, qui s'adresse à des professionnels de l'informatique**. Il est très facile d'en parler, par contre la mise en application des règles de sécurité ne s'improvise pas.
Adressez-vous à de vrais professionnels de la sécurité informatique dont c'est le métier.
On trouvera des filières comme le conseil stratégique de la politique de sécurité, spécialiste en gestion de crise informatique, spécialiste dans la réponse sur incident, ou bien spécialiste dans la collecte de la preuve numérique en post incident.
La sécurité informatique ne permet plus l'amateurisme les enjeux sont trop grands.

Sites utiles

- **Les sites institutionnels :**

https://www.ssi.gouv.fr/ Agence Nationale de la Sécurité des Systèmes d'Information

https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite

- **Les sites de veille du secteur :**

https://www.ihedn.fr/

https://www.observatoire-fic.com/

http://www.cybersecurite-grandsud.fr/

https://www.cyberathack.com/

https://www.fafiec.fr/

http://observatoire-metiers.opiiec.fr/

http://referentiels-metiers.opiiec.fr/

Pour en savoir plus

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

mcefportetmuretain

@mcefpm

POLE EMPLOI
www.pole-emploi.fr/
http://www.emploi-store.fr/

ME FORMER EN REGION
www.meformerenregion.fr/

ONISEP
www.onisep.fr

Remerciements : Mme Sandra JOFFROY
Monsieur Fabrice CRASNIER

Autres parutions de la MCEF Portet-Muretain :

Le guide des métiers du Sanitaire et Social (2017)
Le guide des métiers de l'artisanat d'art (2017)
Le guide des métiers du transport (2017)

MCEF Portet-Muretain
8 Rue de l'hôtel de ville
31120 Portet/Garonne
☎ **05 34 50 16 83**
cdr.mcefportet@orange.fr

Parution : Novembre 2017

UNION EUROPÉENNE — l'Europe s'engage en Occitanie — La Région Occitanie Pyrénées · Méditerranée